What Is Claimed Is:

1. An access privilege transferring method for safely transferring access privileges between clients and between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, comprising the steps of:

(a) causing each of the clients to hold user information and secret information;

(b) causing the server to hold the user information and the secret information of each of the clients;

(c) causing the client to generate privilege information;

(d) causing the client to apply a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information;

(e) causing the client to transmit the user information, the privilege information and the protected privilege information to another client;

(f) causing the another client to transmit the user information, the privilege information and the protected privilege information to the server, thereby making a request to access each object;

(g) causing the server to check to see whether the privilege information received in Step (f) is valid;

(h) causing the server to apply a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information;

(i) causing the server to compare the protected privilege information received in Step (f) with the protected privilege information generated in Step (h); and

(j) allowing an access to each object in response to the coincidence of the two as a result of the comparison in Step (i).

2. The access privilege transferring method according to claim 1, wherein the another client transmits the user information, the privilege information and the protected privilege information received in Step (e) to a second other client.

3. An access privilege transferring method for allowing each of clients activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, to safely transfer access privileges to another client, comprising the steps of:

(a) holding user information and secret information to be shared by at least the server(s);

(b) generating privilege information; and

(c) applying a predetermined calculating operation to information comprising at least the privilege information and the secret information to thereby generate protected privilege information capable of being safely transferred to another client.

4. An access privilege transferring method for allowing each of servers activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects following privilege information held by each of the clients is allowed, to safely respond to an access request issued from the client to which access privileges are transferred, comprising the steps of:

(f) receiving an access request including user information, privilege information and protected privilege information;

(g) checking to see whether the privilege information received in Step (f) is valid;

(h) applying a predetermined calculating operation to information comprising at least privilege information and secret information to thereby generate protected privilege information;

(i) comparing the protected privilege information received in Step (f) with the protected privilege information generated in Step (h); and

(j) allowing an access to each of the objects in response to the coincidence of the two as a result of the comparison in Step (i).

5. The access privilege transferring method according to claim 1, wherein the predetermined calculating operation is to apply a one-way function to a bit string obtained by concatenating operands with one another.

6. An access privilege transferring method for safely transferring access privileges between clients and between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, comprising the steps of:

(A) causing each of the clients to hold user information and secret information;

(B) causing the server to hold the user information and secret information of each of the clients;

(C) causing the client to generate privilege information;

(D) causing the client to apply a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information;

(E) causing the client to transmit the user information, the privilege information and the first protected privilege information to another client;

(F) causing the another client to receive a challenge character string from the server;

(G) causing the another client to apply a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information;

(H) causing the another client to transmit the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access each of the objects;

(I) causing the server to check to see whether the privilege information received in Step (H) is valid;

(J) causing the server to apply a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information;

(K) causing the server to apply a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated in Step (J), thereby generating second protected privilege information;

(L) causing the server to compare the second protected privilege information received in Step (H) with the second protected privilege information generated in Step (K); and

(M) allowing an access to each object in response to the coincidence of the two as a result of the comparison in Step (N).

7. The access privilege transferring method according to claim 6, wherein the another client transmits the user information, the privilege information and the protected

privilege information received in Step (E) to a second other client.

8. An access privilege transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, comprising the steps of:

(F) causing the server to transmit a challenge character string to the client that makes a request to access each of the objects;

(G) causing the client to apply a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information;

(H) causing the client to transmit the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access each of the objects;

(I) causing the server to check to see whether the privilege information received in Step (H) is valid;

(J) causing the server to apply a predetermined calculating operation to information comprising at least the privilege information and secret information, thereby generating first protected privilege information;

(K) causing the server to apply a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated in Step (J), thereby generating second protected privilege information;

(L) causing the server to compare the second protected privilege information received in Step (H) with the second protected privilege information generated in Step (K);

and

(M) causing the server to allow an access to each of the objects in response to the coincidence of the two as a result of the comparison in Step (N).

9. The access privilege transferring method according to claim 6, wherein the predetermined calculating operation is to apply a one-way function to a bit string obtained by concatenating operands with one another.

10. An access privilege transferring method for safely transferring access privileges between clients and between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, comprising the steps of:

(a) causing each of the clients to hold user information and secret information;

(b) causing the server to hold the user information and the secret information of each of the clients;

(c) causing the client to generate privilege information;

(d) causing the client to encrypt the privilege information by using the secret information, thereby generating protected privilege information;

(e) causing the client to transmit the user information and the protected privilege information to another client;

(f) causing the another client to transmit the user information and the protected privilege information to the server, thereby making a request to access each of the objects;

(g) causing the server to decrypt the protected privilege information by using the secret information corresponding to the user information, thereby generating privilege information;

(h) causing the server to check to see whether the privilege information generated in Step (g) is valid; and

(i) allowing an access to each object in accordance with the result of check for validity in Step (h).

11. An access privilege transferring method for allowing each of clients activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, to safely transfer access privileges to another client, comprising the steps of:

(a) holding user information and secret information to be shared by the server(s);

(b) generating privilege information; and

(c) encrypting the privilege information by using the secret information to thereby generate protected privilege information capable of being safely transferred to another client.

12. An access privilege transferring method for allowing each of servers activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects following privilege information held by each of the clients is allowed, to safely respond to an access request issued from the client to which access privileges are transferred, comprising the steps of:

(f) receiving an access request including user information and protected privilege information;

(g) decrypting the protected privilege information by using secret information corresponding to the user information to thereby generate privilege information;

(h) checking whether the privilege information generated in Step (g) is valid; and

(i) allowing an access to each of the objects in accordance with the result of check for validity in Step (h).

13. An access privilege transferring method for safely transferring access privileges between clients and between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, comprising the steps of:

(A) causing each of the clients to hold user information and secret information;

(B) causing the server to hold the user information and the secret information of each of the clients;

(C) causing the client to generate privilege information;

(D) causing the client to encrypt the privilege information by using the secret information, thereby generating first protected privilege information;

(E) causing the client to transmit the user information, the privilege information and the first protected privilege information to another client;

(F) causing the another client to receive a challenge character string from the server;

(G) causing the another client to encrypt the challenge character string by using the first protected privilege information, thereby generating second protected privilege information;

(H) causing the another client to transmit the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access each object;

(I) causing the server to check to see whether the privilege information received in Step (H) is valid;

(J) causing the server to encrypt the privilege information by using the secret information, thereby generating first protected privilege information;

(K) causing the server to encrypt the challenge character string by using the first protected privilege information generated in Step (J), thereby generating second protected privilege information;

(L) causing the server to compare the second protected privilege information received in Step (H) with the second protected privilege information generated in Step (K); and

(M) allowing an access to each object in response to the coincidence of the two as a result of the comparison in Step (N).

14. An access transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by the client is allowed, comprising the steps of:

(F) causing the server to transmit a challenge character string to the client that makes a request to access each of the objects;

(G) causing the client to encrypt the challenge character string by using the first protected privilege information, thereby generating second protected privilege information;

(H) causing the client to transmit the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access each of the objects;

(I) causing the server to check to see whether the privilege information received

in Step (H) is valid;

(J) causing the server to encrypt the privilege information by using secret information, thereby generating first protected privilege information;

(K) causing the server to encrypt the challenge character string by using the first protected privilege information generated in Step (J), thereby generating second protected privilege information;

(L) causing the server to compare the second protected privilege information received in Step (H) with the second protected privilege information generated in Step (K); and

(M) causing the server to allow an access to each of the objects in response to the coincidence of the two as a result of the comparison in Step (N).

15. An information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit secret information to a second client;

causing the first client to transmit an encryption key to the second client; and

causing the second client to encrypt the secret information by using the encryption key, thereafter storing the encrypted secret information in a secondary memory device.

16. An information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to encrypt the secret information by using an encryption key,

thereby generating protected secret information;

causing the first client to transmit the protected secret information to a second client;

causing the second client to store the protected secret information in a secondary memory device;

causing the first client to transmit a decryption key for decrypting the information encrypted by the encryption key to the second client; and

causing the second client to decrypt the protected secret information by using the decryption key, thereby obtaining the secret information.

17. The information managing method according to claim 16, wherein the encryption key is identical to the decryption key.

18. An information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit secret information to a second client;

causing the second client to hold an encryption key for encrypting information and a decryption key for decrypting the encrypted information encrypted by the encryption key;

causing the second client to transmit the decryption key to the first client;

causing the second client to store protected secret information obtained by encrypting the secret information with the encryption key in a secondary memory device; and

causing the second client to decrypt the protected secret information by using the decryption key, thereby obtaining the secret information.

19. An information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit first secret information to a second client;

causing the second client to transmit a challenge character string to the first client;

causing the first client to apply a predetermined calculating operation to the challenge character string and second secret information, thereby generating an encryption key;

causing the first client to transmit the encryption key to the second client; and

causing the second client to store protected secret information obtained by encrypting the secret information by using the encryption key in a secondary memory device.